

PAT-NO: JP409045008A
DOCUMENT- JP 09045008 A
IDENTIFIER:
TITLE: DATA TRANSMITTING METHOD, DATA RECORDING APPARATUS,
DATA RECORDING MEDIUM AND DATA REPRODUCING APPARATUS

PUBN-DATE: February 14, 1997

INVENTOR-INFORMATION:

NAME	COUNTRY
SAKO, YOICHIRO	
OSAWA, YOSHITOMO	
KURIHARA, AKIRA	
KAWASHIMA, ISAO	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SONY CORP	N/A

APPL-NO: JP07195191
APPL-DATE: July 31, 1995

INT-CL G11B020/12 , G06F012/14 , G06F012/16 , G09C001/00 ,
(IPC): H03M013/00 , H04L001/00 , H04L009/18

ABSTRACT:

PROBLEM TO BE SOLVED: To encrypt data in a simple constitution and access at high speed.

SOLUTION: In an error-correcting code format, a sector 73 is constituted of a head part 71 and a user data part 72. An error correction C1 direction is set in a R/W direction and a C1 parity 74 is generated and added. On the other hand, an error correction C2 direction is set in a direction oblique to the C1 direction and a C2 parity 75 is generated and added. Data excluding at least the head part 71, e.g., a part 76 in the same row as the head part 71 among the

data handled in an error-correcting code process are converted in
00005000CA with an encryption flag data.

COPYRIGHT: (C)1997,JPO

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-45008

(43)公開日 平成9年(1997)2月14日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/12	1 0 2	9295-5D	G 1 1 B 20/12	1 0 2
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
	3 2 0	7623-5B		3 2 0 A
G 0 9 C 1/00	6 6 0	7259-5J	G 0 9 C 1/00	6 6 0 D
H 0 3 M 13/00			H 0 3 M 13/00	

審査請求 未請求 請求項の数7 OL (全 15 頁) 最終頁に続く

(21)出願番号 特願平7-195191

(22)出願日 平成7年(1995)7月31日

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 佐古 曜一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 栗原 章

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 弁理士 小池 晃 (外2名)

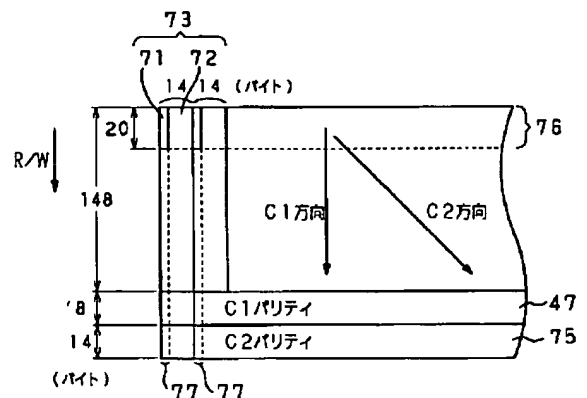
最終頁に続く

(54)【発明の名称】 データ伝送方法、データ記録装置、データ記録媒体及びデータ再生装置

(57)【要約】

【課題】 簡単な構成で暗号化を施すと共に、高速アクセスを可能とする。

【解決手段】 誤り訂正符号フォーマットにおいて、ヘッダ部71とユーザデータ部72とでセクタ73が構成されており、R/W方向に誤り訂正のC1方向がとられてC1パリティ74が生成付加され、これに対して斜めの方向に誤り訂正のC2方向がとられてC2パリティ75が生成付加される。この誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部71を除いたデータ、例えばヘッダ部71と同一行の部分76を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施す。



【特許請求の範囲】

【請求項1】 データの伝送単位がヘッダ部とユーザデータ部とを有して成る入力デジタルデータに誤り訂正符号化処理を施して伝送するデータ伝送方法において、上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除いたデータに対して、暗号化の鍵情報に応じてデータ変換を施すことを特徴とするデータ伝送方法。

【請求項2】 上記データ変換は、データと暗号化の鍵情報との論理演算により行われることを特徴とする請求項1記載のデータ伝送方法。

【請求項3】 上記暗号化の鍵情報は、少なくとも一部に識別情報を含むことを特徴とする請求項1記載のデータ伝送方法。

【請求項4】 上記データ変換が行われるデータは、上記誤り訂正符号のマトリクスにおける上記ヘッダ部と同一行あるいは同一列のデータを除いたデータであることを特徴とする請求項1記載のデータ伝送方法。

【請求項5】 データの記録単位がヘッダ部とユーザデータ部とを有して成る入力デジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録装置において、

暗号化の鍵情報の入力手段と、

この入力手段からの鍵情報に応じて、上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対してデータ変換を施す手段とを有することを特徴とするデータ記録装置。

【請求項6】 データの記録単位がヘッダ部とユーザデータ部とを有して成る入力デジタルデータに誤り訂正符号化処理を施す際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対して、暗号化の鍵情報に応じてデータ変換が施されて得られた信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項7】 データの記録単位がヘッダ部とユーザデータ部とを有して成る入力デジタルデータに対して誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生装置において、

上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対して施されるデータ変換を示す暗号化の鍵情報を入力する鍵情報入力手段と、

上記誤り訂正符号化処理に対応する誤り訂正復号化処理を行うと共に、上記鍵情報入力手段からの暗号化の鍵情報に応じたデータに上記データ変換に対する復号化のためのデータ変換を施す誤り訂正復号化手段とを有することを特徴とするデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コピー防止や不正使用の阻止、あるいは課金システムに適用可能なデータ

伝送方法、データ記録装置、データ記録媒体、及びデータ再生装置に関する。

【0002】

【従来の技術】近年において、光ディスク等のデジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、デジタルオーディオデータやデジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる弊害が生じてきているのが実情である。

【0003】デジタルオーディオデータやデジタルビデオデータの不法コピー等を回避するためには、例えばいわゆるSCMS（シリアルコピー管理システム）やCGMS（コピー世代管理システム）の規格が知られているが、これは記録データの特定部分にコピー禁止フラグを立てるようなものであるため、いわゆるダンプコピー等の方法によりデータを抜き出される問題がある。

【0004】また、コンピュータデータ等のファイル内容自体を暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。これは、情報流通の形態として、情報が暗号化されて記録されたデジタル記録媒体を配布したり、暗号化されたデジタル信号を有線、無線の伝送路を介して容易に入手可能にしておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものであるが、簡単で有用な暗号化の手法の確立が望まれている。

【0005】

【発明が解決しようとする課題】ところで、データの暗号化の際に、データ記録単位あるいは伝送単位となるセクタのヘッダ部分の同期（シンク）やアドレスのデータが暗号化されていると、暗号を解かないと同期やアドレスの情報が得られないため、高速アクセスの障害となることがある。

【0006】本発明は、上述したような実情に鑑みてなされたものであり、簡単な構成で暗号化が行え、暗号の難易度あるいは深度の制御も容易に行え、また、高速アクセス性の劣化等の弊害も生じないようなデータ伝送方法、データ記録装置、データ記録媒体、及びデータ再生装置の提供を目的とする。

【0007】

【課題を解決するための手段】上記の課題を解決するために、本発明は、誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施すことを特徴としている。このデータ変換としては、データと上記鍵情報との論理演算を挙げることができる。上記鍵情報の一部に媒体や装置等の識別情報を含ませてもよい。

なお、上記ヘッダ部とは、データ伝送単位あるいは記録単位となる例えばセクタの先頭位置に配置されている部分で、セクタシンクやセクタアドレス等を含むものである。

【0008】また、本発明に係るデータ記録媒体は、誤り訂正符号化処理を施す際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換が施されて得られた信号が記録されて成ることを特徴としている。

【0009】さらに、本発明に係るデータ再生方法は、誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換が施されており、対応する誤り訂正復号化処理の際に取り扱われるデータの内の上記暗号化の鍵情報に応じたデータに上記データ変換に対する復号化のためのデータ変換を施すことを特徴としている。

【0010】誤り訂正符号化処理の際に取り扱われるデータのヘッダ部を除くデータに対して、暗号化の鍵情報に応じたデータ変換を施すことにより、ヘッダ部については暗号化の復号化処理を介さずに再生できる。再生時に鍵情報に応じた暗号の復号化のためのデータ変換を施さないと、訂正不能誤りの個数が増加する。データ変換を施すデータの個数を変化させることにより、所望の暗号化の難易度を実現できる。

【0011】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しながら説明する。

【0012】図1は、本発明の実施の形態が適用されるデータ記録装置を概略的に示すブロック図である。この図1において、入力端子11には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、インターフェース回路12を介して、セクタ化回路13に送られ、所定データ量単位、例えば2048バイト単位でセクタ化される。セクタ化されたデータは、スクランブル処理回路14に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路15に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路16に送られる。誤り訂正符号化回路16では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路17では、所定の変調方式に従って、例えば8ビットデータを16チャンネルビットの変調データに変換し、同期付加回路1

8に送る。同期付加回路18では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブロールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ19を介して記録ヘッド20に送っている。記録ヘッド20は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体21に上記変調された記録信号の記録を行う。このディスク状記録媒体21は、スピンドルモータ22により回転駆動される。

【0013】なお、上記スクランブル処理回路14は、ヘッダ付加回路15の後段に挿入して、ヘッダ付加されたディジタルデータに対してスクランブル処理を施して誤り訂正符号化回路16に送るようにしてもよい。

【0014】ここで、上記誤り訂正符号化回路16は、誤り訂正符号化処理の際に取り扱われるデータの内の上記ヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施すような構成を有している。

【0015】この誤り訂正符号化回路16の構成の具体例を図2、図3に示す。これらの図2、図3において、入力端子51には、上記図1のヘッダ付加回路15からのデータが第1の符号化器であるC1エンコーダ52に供給されている。この具体例においては、誤り訂正符号化の1フレームは148バイトあるいは148シンボルのデータから成るものとしており、入力端子51からのディジタルデータが148バイト毎にまとめられて、第1の符号化器であるC1エンコーダ52に供給される。C1エンコーダ52では8バイトのPパリティが付加され、インターリーブのための遅延回路53を介して第2の符号化器であるC2エンコーダ54に送られる。C2エンコーダ54では14バイトのQパリティが付加され、このQパリティは遅延回路55を介してC1エンコーダ52に帰還されている。このC1エンコーダ52からのP、Qパリティを含む170バイトが取り出されて、遅延回路56を介し、図3のインバータ部57aを有する再配列回路57を介して出力され、図1の変調回路17に送られる。

【0016】このような誤り訂正符号化回路において、内部で取り扱われるデータの内のヘッダ部を除いたデータに対して、暗号化の鍵情報に応じてデータ変換を施すような暗号化処理としては、例えば再配列回路57内のインバータ部57aの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、22バイトのP、Qパリティに対して再配列回路57のインバータ部57aによる反転が行われて出力されるが、これらのインバータ部57a内のインバータのいくつかを無くしたり、C1データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。

【0017】このようなデータ変換を施す場合、基準構

成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばC1エンコードについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが9であるため、最大4バイトまでのエラー検出訂正が行え、消失(イレージャ)ポイントがあれば最大8バイトまでの訂正が可能であることから、違いが5箇所以上あると、C1符号では常に訂正不可となる。違いが4箇所の場合は、他に1バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが3、2、1箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【0018】この場合、予めインバータの変更を行う場所を例えば2箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を2箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【0019】さらに、インバータの挿入あるいは変更位置としては、図2の再配列回路57の位置に限定されず、例えばC1エンコード52の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、上記データ変換としては、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしたり、データを暗号化の鍵情報に応じて転置するようになり、データを暗号化の鍵情報に応じて置換するようにしてもよい。

【0020】次に、上記誤り訂正符号化回路で取り扱われるデータの内のヘッダ部について説明する。

【0021】図4はセクタフォーマットの具体例を示しており、1セクタは、2048バイトのユーザデータ領域41に対して、4バイトの同期領域42と、16バイトのヘッダ領域43と、4バイトの誤り検出符号(EDC)領域44とが付加されて構成されている。誤り検出符号領域44の誤り検出符号は、ユーザデータ領域41及びヘッダ領域43に対して生成される32ビットのCRC符号から成っている。

【0022】ヘッダ領域43内には、図4に示すように、いわゆる巡回符号であるCRC45、コピーの許可/不許可やコピー世代管理等のためのコピー情報46、多層ディスクのどの層かを示す層(レイヤ)47、アドレス48、予備49の各領域が設けられている。

【0023】ここで、本発明の実施の形態におけるヘッダ部は、同期すなわちセクタシンクとヘッダ情報とを含

むものであり、上記図4の例では、4バイトの同期領域42と16バイトのヘッダ領域43との計20バイトのデータがヘッダ部のデータである。残りのユーザデータ領域41及び誤り検出符号(EDC)領域44がユーザデータ部となる。

【0024】このようなヘッダ部とユーザデータ部に対して、クロスインターリーブ型の誤り訂正符号化を施すときの誤り訂正フォーマットを図5に示す。

【0025】この図5の例は、上記図4のセクタフォーマットのデータを上記図2、図3の誤り訂正符号化回路にて誤り訂正符号化処理するときの様子を示し、20バイトのヘッダ部71と2052バイトのユーザデータ部72とで、2072バイトのセクタ73が構成されている。このセクタは、記録/再生方向であるR/W方向に148バイト、これと直交する方向に14バイトの2次元に配列され、R/W方向に誤り訂正のC1方向がとられて8バイトのC1パリティ74が生成付加され、これに対して斜めの方向に誤り訂正のC2方向がとられて14バイトのC2パリティ75が生成付加されている。この図5の誤り訂正フォーマットのR/W方向の先頭20バイトのヘッダ部71と同一行の部分76を除いた部分に対して、上記データ変換を行っている。なお、図5のヘッダ部71と同一列の部分77を除いた部分に対して、上記データ変換を行わせてもよく、これらを組み合わせるようにしてもよい。

【0026】ここで図6は、上記誤り訂正符号化回路16の他の具体例として、再配列回路57内のインバータ部57aの後段すなわち出力側の位置に、データ変換手段としての排他的論理和(ExOR)回路群61を挿入し、C1エンコード52の前段すなわち入力側の位置にも、データ変換手段としてのExOR回路群66を挿入した例を示している。

【0027】これらのデータ変換手段としてのExOR回路群61、66は、誤り訂正フォーマットの上記図5の部分76に相当する20バイト分を除くデータに対してデータ変換を行うものである。具体的に、ExOR回路群61は、C1エンコード52から遅延回路56、及び上記再配列回路57のインバータ部57aを介して取り出される170バイトのデータ、すなわち情報データC1

170n+169~C1170n+22 及びパリティデータP1
170n+21 ~P1170n+14、Q1170n+13 ~Q1170nの
内、先頭の20バイトのデータC1170n+169~C1
170n+150を除いた残り150バイトのデータC1
170n+149~Q1170nに対して排他的論理和(ExOR)回路を用いたデータ変換を行い、ExOR回路群66は、148
バイトの入力データB148n~B148n+147の内、先頭の20
バイトのデータB148n~B148n+19を除いた残り128
バイトのデータB148n+20 ~B148n+147に対して排他
的論理和(ExOR)回路を用いたデータ変換を行う。これ
らのExOR回路群61、66に用いられるExOR回路は、1

バイトすなわち8ビットの入力データと1ビットの制御データで指示される所定の8ビットデータとの排他的論理和 (ExOR) をそれぞれとるような8ビットExOR回路であり、このような8ビットExOR回路 (所定の8ビットデータがオール1の場合はインバート回路に相当する) が、ExOR回路群61では150個、ExOR回路群66では128個用いられている。

【0028】この図6においては、150ビットの鍵情報が端子62に供給され、いわゆるDラッチ回路63を介してExOR回路群61内の150個の各ExOR回路にそれぞれ供給されている。Dラッチ回路63は、イネーブル端子64に供給された1ビットの暗号化制御信号に応じて、端子62からの150ビットの鍵情報をそのままExOR回路群61に送るか、オールゼロ、すなわち150ビットの全てを“0”とするかが切換制御される。ExOR回路群61の150個の各ExOR回路の内、Dラッチ回路63から“0”が送られたExOR回路は、上記再配列回路57の内のインバート部57aからのデータをそのまま出力し、Dラッチ回路63から“1”が送られたExOR回路は、上記再配列回路57のインバート部57aからのデータを交換して出力する。オールゼロのときには、上記再配列回路57のインバート部57aからのデータをそのまま出力することになる。また、ExOR回路群66については、128個のExOR回路を有し、鍵情報が128ビットであること以外は、上記ExOR回路群61の場合と同様であり、端子67に供給された128ビットの鍵情報がDラッチ回路68を介してExOR回路群66内の128個のExOR回路にそれぞれ送られると共に、Dラッチ回路68はイネーブル端子69の暗号化制御信号により128ビットの鍵情報がオールゼロかが切換制御される。

【0029】この図6の例において、ExOR回路群61は、C1エンコード52から遅延回路56、インバート部57aを介して取り出される170バイトのデータとしての情報データC1170n+169～C1170n+22及びパリティデータP1170n+21～P1170n+14、Q1170n+13～Q1170nの内、先頭の20バイトのデータC1170n+169～C1170n+150を除いた残り150バイトのデータC1170n+149～Q1170nに対して排他的論理和 (ExOR) 回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り128バイトの情報データC1170n+149～C1170n+22に対して、128ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【0030】この図6の回路においても、上記図2、図3の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群61、66のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【0031】なお、上記データ変換手段としてのExOR回路群61、66の代わりに、AND、OR、NAND、

NOR、インバート回路群等を使用してもよい。また、8ビット単位で1ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8ビットの情報データに対して8ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの1ワードに相当する8ビットの内の各ビットに対してそれぞれAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用してもよい。この場合には、例えば128バイトすなわち128×8ビットのデータに対して、128×8ビットの鍵データが用いられることになり、さらにAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。

【0032】また、上述した実施の形態においては、クロスインターリーブ型の誤り訂正符号の例について説明したが、図7に示すような積符号の場合にも同様に適用可能である。

【0033】この図7の例においては、20バイトのヘッダ部81と2052バイトのユーザデータ部82とから成るセクタ83の8セクタ分を、縦148バイト、横112バイトの2次元マトリクス構成とし、読み出し/書き込み方向であるR/W方向の148バイトに対してC1パリティ84を生成付加し、これに直交する方向の112バイトに対してC2パリティ85を生成付加している。これらのC1、C2パリティの交差する部分86は、C1符号化とC2符号化とが2重にかかっている。また、20バイトのヘッダ部81と同一行の図中斜線を付した部分87を除いたデータに対して、上記鍵情報に応じたデータ変換を施すようにする。

【0034】また、この積符号の場合にも、ヘッダ部81と同一列の部分88を除いたデータに対して、上記鍵情報に応じたデータ変換を施すようにしてもよく、さらに、ヘッダ部81と同一行の部分87及び同一列の部分88の両方を除いた部分に対してのみ、上記鍵情報に応じたデータ変換を施すようにしてもよい。

【0035】ここで、積符号の場合には、ヘッダ部81と同一行の図中斜線を付した部分87の全てを除かなくとも、ヘッダ部81のみを除くことができ、このヘッダ部81のみを除いた残りのデータに対して上記データ変換を行うようにしてもよい。なお、C1パリティのないものがLDC (ロングディスタンスコード) であり、これを誤り訂正符号に用いてもよい。

【0036】このように、誤り訂正符号化の際に取り扱われる中間データ等について、暗号化の鍵情報に応じた一部のデータに対してインバート等でデータ変換を施すことにより、訂正不能誤りの発生確率が変化し、データ変換を施すデータ数に応じて暗号化のレベル、深度、解読の困難さ等が変化することになる。すなわち、用途に

応じて必要とされる暗号化の深度や難易度を、データ変換を施すデータ数により任意に設定でき、概要をサンプルとして提供したい場合や、正規ユーザ以外には再生不可能としたい場合や、セキュリティレベルの要求等に応じて種々の対応が図れる。

【0037】また、セクタの先頭部分のヘッダ部については、上記データ変換が施されないため、セクタシンクやセクタアドレスの読み取りが迅速に行え、高速アクセスが可能である。

【0038】ここで、上記誤り訂正符号化回路16のみならず、上記図1のセクタ化回路13、スクランブル処理回路14、ヘッダ付加回路15、変調回路17、及び同期付加回路18のいずれか少なくとも1つの回路は、入力に対して暗号化処理を施して出力するような構成を有することが挙げられる。このような暗号化処理の鍵情報は、記録媒体21のデータ記録領域とは別の領域に書き込まれた識別情報、例えば媒体固有の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、外部から供給される識別情報等を少なくとも一部に用いている。このように、媒体のデータ記録領域以外に書き込まれる識別情報は、例えば上記インターフェース回路12からTOC (Table of contents) 生成回路23を介して端子24に送られる情報であり、また、インターフェース回路12から直接的に端子25に送られる情報である。これらの端子24、25からの識別情報が、暗号化の際の鍵情報の一部として用いられ、回路13～18の少なくとも1つ、好ましくは2以上で、この鍵情報を用いた入力データに対する暗号化処理が施される。

【0039】この場合、回路13～18のどの回路において暗号化処理が施されたかも選択肢の1つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、1つの回路で暗号化処理が施されていれば、6つの選択肢の1つを選ぶことが必要となり、2つの回路で暗号化処理が施されていれば、30個の選択肢の1つを選ぶことが必要となる。6つの回路13～18の内の1～6つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。

【0040】また、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることで、暗号化のレベルあるいは暗号の解き難さをさらに高めることができる。

【0041】次に、図8は、記録媒体の一例としての光ディスク等のディスク状記録媒体101を示している。このディスク状記録媒体101は、中央にセンタ孔102を有しており、このディスク状記録媒体101の内周から外周に向かって、プログラム管理領域であるTOC (table of contents) 領域となるリードイン (leadin

) 領域103と、プログラムデータが記録されたプログラム領域104と、プログラム終了領域、いわゆるリードアウト (lead out) 領域105とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域104にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域103で管理される。

【0042】上記鍵情報の一部として、データ記録領域であるプログラム領域104以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、TOC領域であるリードイン領域103や、リードアウト領域105に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにすると共に、これを鍵情報として、上述した6つの回路13～18の少なくとも1つ、好ましくは2つ以上で暗号化処理を施して得られた信号をデータ記録領域であるプログラム領域104に記録するようにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域103よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【0043】暗号化としては、上記誤り訂正符号化の際のデータ変換が必ず用いられており、上記ヘッダ部を除くデータに対してのみ暗号化の鍵情報に応じてデータ変換が施されることは勿論である。

【0044】次に、本発明のデータ再生方法が適用されるデータ再生装置について、図9を参照しながら説明する。

【0045】図9において、記録媒体の一例としてのディスク状記録媒体101は、スピンドルモータ108により回転駆動され、光学ピックアップ装置等の再生ヘッド装置109により媒体記録内容が読み取られる。

【0046】再生ヘッド装置109により読み取られたデジタル信号は、TOCデコーダ111及びアンプ112に送られる。TOCデコーダ111からは、ディスク状記録媒体101の上記リードイン領域103にTOC情報の一部として記録された上記識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報が読み取られ、この識別情報が暗号を復号化するための鍵情報の少なくとも一部として用いられる。この他、再生装置内部のCPU122から、再生装置固有の識別情報や、外部からの識別情報を出力するようにし、この識別情報を鍵情報の少なくとも一部として用いるようにしてもよい。なお、外部からの識別

情報としては、通信回線や伝送路等を介して受信された識別情報や、いわゆるICカード、ROMカード、磁気カード、光カード等を読み取って得られた識別情報等が挙げられる。

【0047】再生ヘッド装置109からアンプ112を介し、PLL（位相ロックループ）回路113を介して取り出されたデジタル信号は、同期分離回路114に送られて、上記図1の同期付加回路18で付加された同期信号の分離が行われる。同期分離回路114からのデジタル信号は、復調回路115に送られて、上記図1の変調回路17の変調を復調する処理が行われる。具体的には、16チャンネルビットを8ビットのデータに変換するような処理である。復調回路115からのデジタルデータは、誤り訂正符号化回路116に送られて、図1の誤り訂正符号化回路16での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路117によりセクタに分解され、ヘッダ分離回路118により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路117及びヘッダ分離回路118は、上記図1のセクタ化回路13及びヘッダ付加回路15に対応するものである。次に、デスクランブル処理回路119により、上記図1のスクランブル処理回路14におけるスクランブル処理の逆処理としてのデスクランブル処理が施され、インターフェース回路120を介して出力端子121より再生データが取り出される。

【0048】ここで、上述したように、記録時には、上記図1のセクタ化回路13、スクランブル処理回路14、ヘッダ付加回路15、誤り訂正符号化回路16、変調回路17、及び同期付加回路18の内の、誤り訂正符号化回路16を含むいずれか少なくとも1つの回路において暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路114～119にて、暗号を復号化する処理が必要とされる。すなわち、上記図1のセクタ化回路13にて暗号化処理が施されている場合には、セクタ分解回路117にて暗号化の際の鍵情報を用いた暗号の復号化処理が必要とされる。以下同様に、図1のスクランブル処理回路14での暗号化処理に対応してデスクランブル処理回路119での暗号復号化処理が、図1のヘッダ付加回路15での暗号化処理に対応してヘッダ分離回路118での暗号復号化処理が、それぞれ必要とされる。図1の誤り訂正符号化回路16での暗号化処理は必ずなされており、これに対応して誤り訂正復号化回路116での暗号復号化処理が必要とされる。また、図1の変調回路17で暗号化処理が施されている場合には、これに対応して復調回路115での暗号復号化処理が、さらに図1の同期付加回路18での暗号化処理が施されている場合に対応しては同期分離回路114での暗号復号化処理が、それぞれ必要とされる。

【0049】ここで、誤り訂正復号化回路116では、例えば上記図2、図3の誤り訂正符号化処理の逆処理

が、図10、図11の構成により行われる。

【0050】これらの図10、図11において、上記復調回路115にて復調されたデータの170バイトあるいは170シンボルを1まとまりとして、入力端子141に入力され、図11のインバータ部142aを有する再配列回路142を介し、遅延回路143を介して第1の復号器であるC1デコード144に送られている。このC1デコード144に供給される170バイトのデータの内22バイトがP、Qパリティであり、C1デコード144では、これらのパリティデータを用いた誤り訂正復号化が施される。C1デコード144からは、170バイトのデータが出力されて、遅延回路145を介して第2の復号器であるC2デコード146に送られ、パリティデータを用いた誤り訂正復号化が施される。C2デコード146からの出力データは、図10の遅延・C1デコード回路140に送られる。これは、上記遅延回路143及びC1デコード144と同様のものであり、これらの遅延回路143及びC1デコード144と同様の処理を繰り返すことにより誤り訂正復号化を行うものである。図11の例では、遅延回路147及び第3の復号器であるC3デコード148で表している。この遅延回路147及びC3デコード148、あるいは遅延・C1デコード回路140で最終的な誤り訂正復号化が施され、パリティ無しの148バイトのデータが出力端子149を介して取り出される。この148バイトのデータは、上記図2、図3のC1エンコード52に入力される148バイトのデータに相当するものである。

【0051】そして、図2、図3の誤り訂正符号化回路の再配列回路57のインバータ部57aで、インバータの有無による暗号化、すなわち、鍵情報に応じたデータ変換により、図10、図11の誤り訂正復号化回路の再配列回路142内のインバータ部142aにて、対応する暗号復号化を行うことが必要とされる。ただし、上記データ変換は、ヘッダ部を除くデータに対してのみ施されているため、復号化もヘッダ部を除くデータに対してのみ行われる。その他、図2、図3と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【0052】次に、図12は、上記図6の誤り訂正符号化回路の具体的な構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【0053】この図12において、上記図6の再配列回路57の出力側に挿入されたExOR回路群61に対応して、再配列回路142のインバータ部142aの入力側及び遅延回路143の入力側の位置に、ExOR回路群151が挿入され、図6のC1エンコード52の入力側に挿入されたExOR回路群66に対応して、C3デコード148の出力側にExOR回路群156が挿入されている。

【0054】これらのExOR回路群151、156は、上述したように、セクタのヘッダ部を除くデータに対する

データ変換を復号化するためのデータ変換を施すものであり、ExOR回路群151は、150個の8ビットExOR回路により、またExOR回路群156は、128個の8ビットExOR回路によりそれぞれ構成されている。なお、記録側の図6の誤り訂正符号化回路のExOR回路群61で、パリティデータを除く128バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR回路群151は128個の8ビットExOR回路により構成されることは勿論である。

【0055】この図12の端子152には、図6の端子62に供給される鍵情報に相当する150ビットの鍵情報が供給され、いわゆるDラッチ回路153を介してExOR回路群151内の150個の各ExOR回路にそれぞれ供給されている。Dラッチ回路153は、イネーブル端子154に供給された1ビットの暗号化制御信号に応じて、端子152からの150ビットの鍵情報をそのままExOR回路群151に送るか、オールゼロ、すなわち150ビットの全てを“0”とするかが切換制御される。また、ExOR回路群156については、128個のExOR回路を有し、鍵情報が図6の端子67に供給される鍵情報と同様の128ビットであること以外は、上記ExOR回路群151の場合と同様であり、端子157に供給された128ビットの鍵情報がDラッチ回路158を介してExOR回路群156内の128個のExOR回路にそれぞれ送られると共に、Dラッチ回路158はイネーブル端子159の暗号化制御信号により128ビットの鍵情報がオールゼロかが切換制御される。

【0056】このように、誤り訂正回路のインバータを暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータの数を制御することにより、絶対再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータやExOR回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な絶対再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように1箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆるLSIやICチップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【0057】また、セクタのヘッダ部のデータに対してはデータ変換が施されないため、再生時にヘッダ部内のセクタシンク（同期）やセクタアドレスについての暗号化の復号化のためのデータ変換が不要となり、高速ア

セスが可能である。

【0058】なお、本発明は、上記実施例のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、この他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【0059】

【発明の効果】本発明によれば、誤り訂正符号化処理の際に取り扱われるデータの内のヘッダ部を除くデータに対して、暗号化の鍵情報に応じてデータ変換を施しているため、再生時にヘッダ部の暗号化を解く処理が不要となり、ヘッダ部のデータが迅速に得られるため、高速アクセスが可能である。また、誤り訂正処理である程度データ復元が可能な状態から、データ復元が行えない状態までの任意のレベルの暗号化が行える。これによって、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、データ提供の用途に応じた、あるいはセキュリティレベルに応じた対応が可能となる。

【0060】さらに、誤り訂正処理の中で鍵のビット数の大きな暗号化が可能であり、誤り訂正符号化や復号化ICあるいはLSIのような巨大なブラックボックスの中で暗号化を実現しているため、一般ユーザによる解読を困難化し、データセキュリティを大幅に向上させることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態が適用可能なデータ記録装置の概略構成を示すブロック図である。

【図2】誤り訂正符号化回路の一例の概略構成を示す図である。

【図3】誤り訂正符号化回路の一例の具体的な構成を示す図である。

【図4】セクタフォーマットの一例を示す図である。

【図5】クロスインターリーブ型誤り訂正符号の一例を示す図である。

【図6】誤り訂正符号化回路の他の具体例を示す図である。

【図7】積符号の場合の誤り訂正符号の一例を示す図である。

【図8】データ記録媒体の一例を示す図である。

【図9】本発明の実施の形態が適用可能なデータ再生装置の概略構成を示すブロック図である。

【図10】誤り訂正復号化回路の一例の概略構成を示す図である。

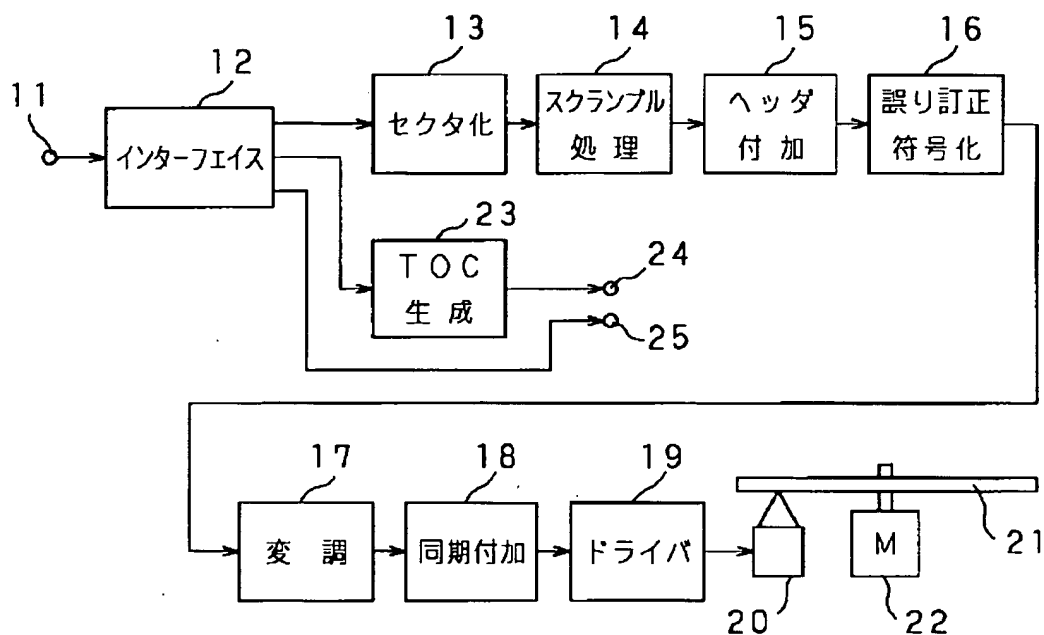
【図11】誤り訂正復号化回路の一例の具体的な構成を示す図である。

【図12】誤り訂正復号化回路の他の例を示す図である。

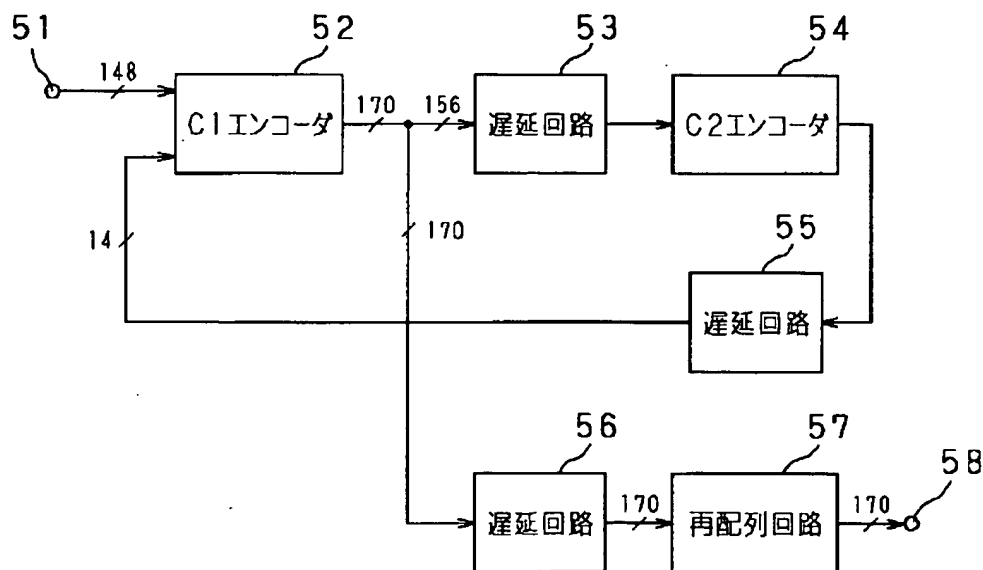
【符号の説明】

- | | |
|---------------------------|-----------------------|
| 13 セクタ化回路 | 57、142 再配列回路 |
| 14 スクランブル処理回路 | 57a、142a インバータ部 |
| 15 ヘッド付加回路 | 61、66、151、156 ExOR回路群 |
| 16 誤り訂正符号化回路 | 114 同期分離回路 |
| 17 変調回路 | 115 復調回路 |
| 18 同期付加回路 | 116 誤り訂正復号化回路 |
| 52 C1エンコーダ | 117 セクタ分解回路 |
| 53、55、56、143、145、147 遅延回路 | 118 ヘッド分離回路 |
| 54 C2エンコーダ | 119 デスクランブル処理回路 |

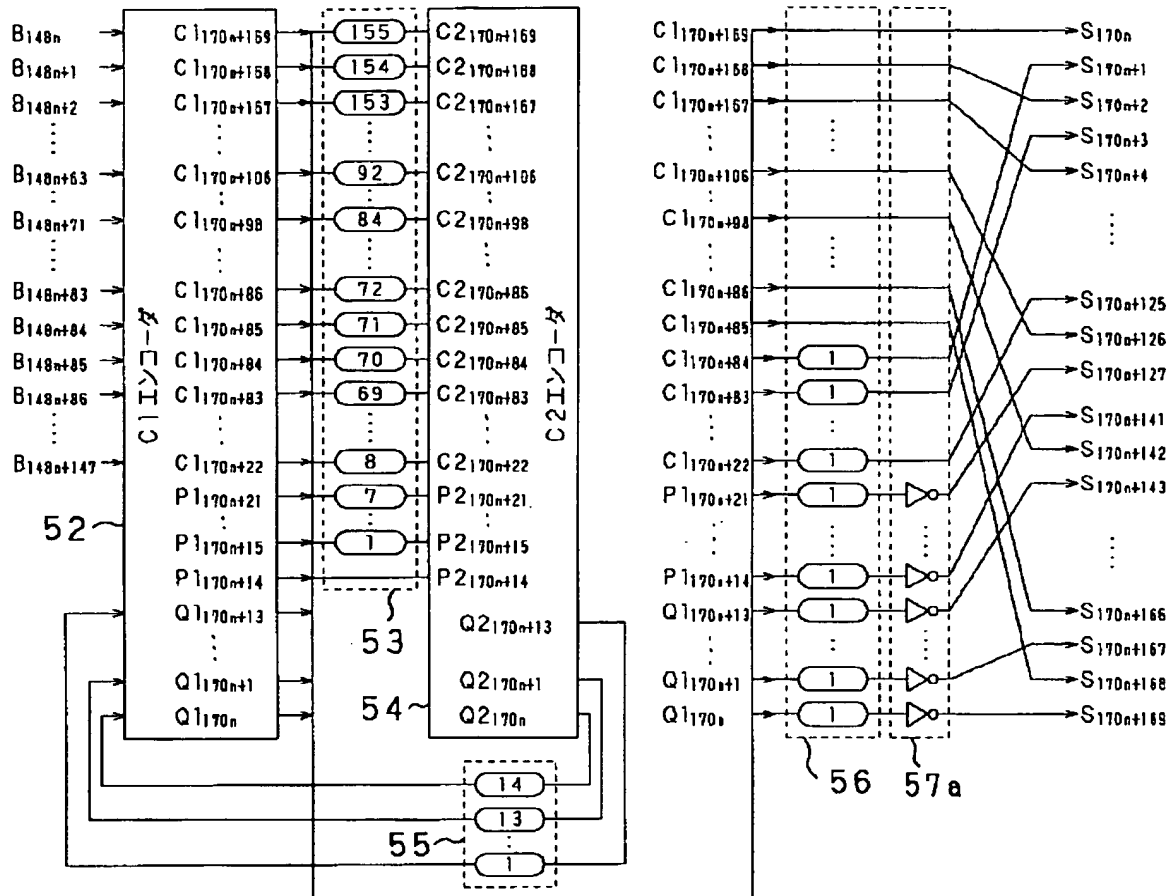
【図1】



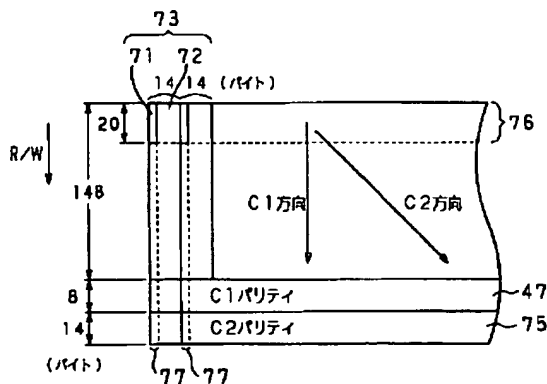
【図2】



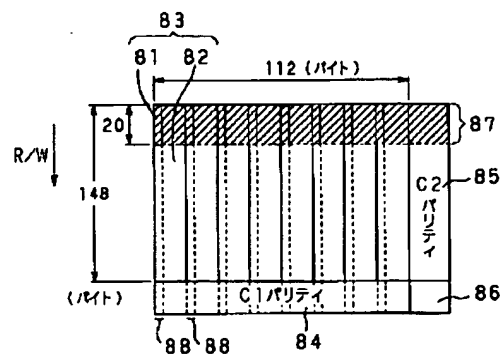
【図3】



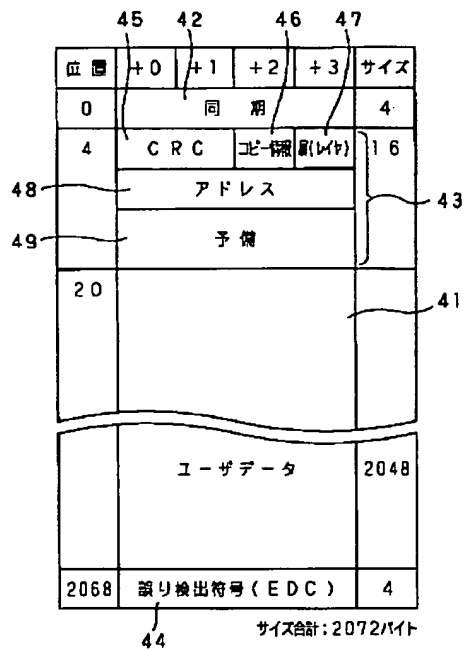
【図5】



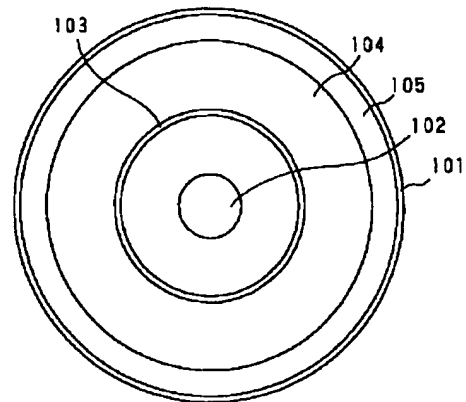
【図7】



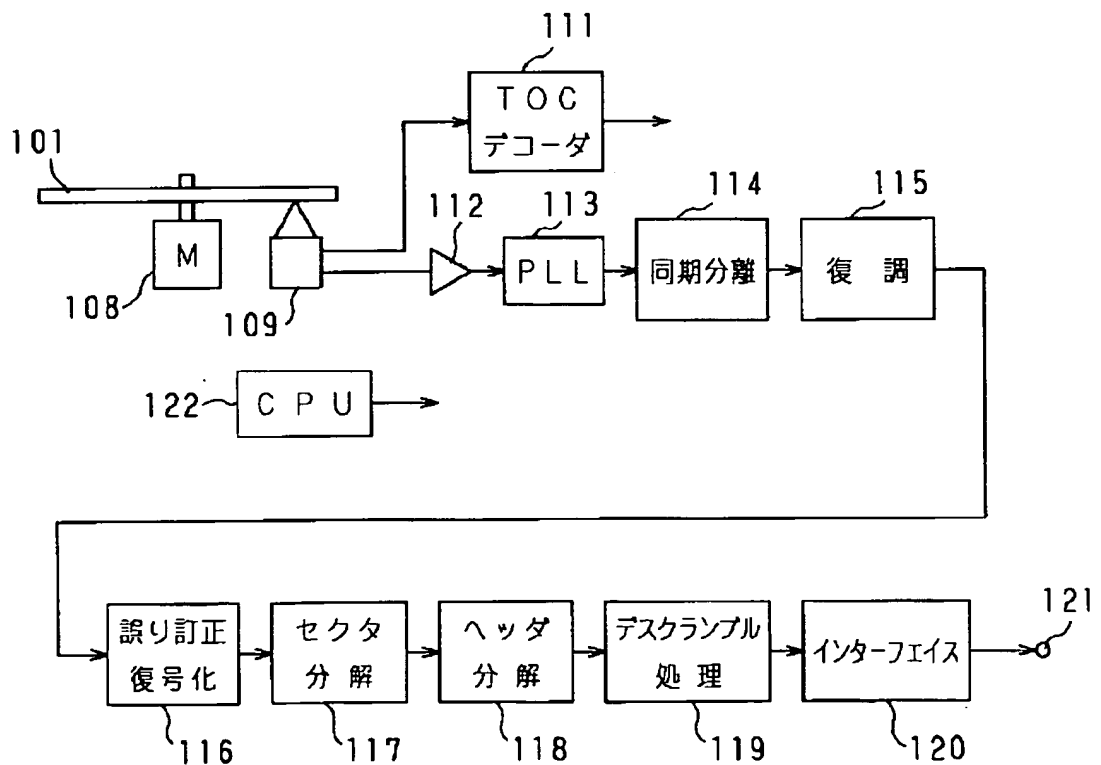
【図4】



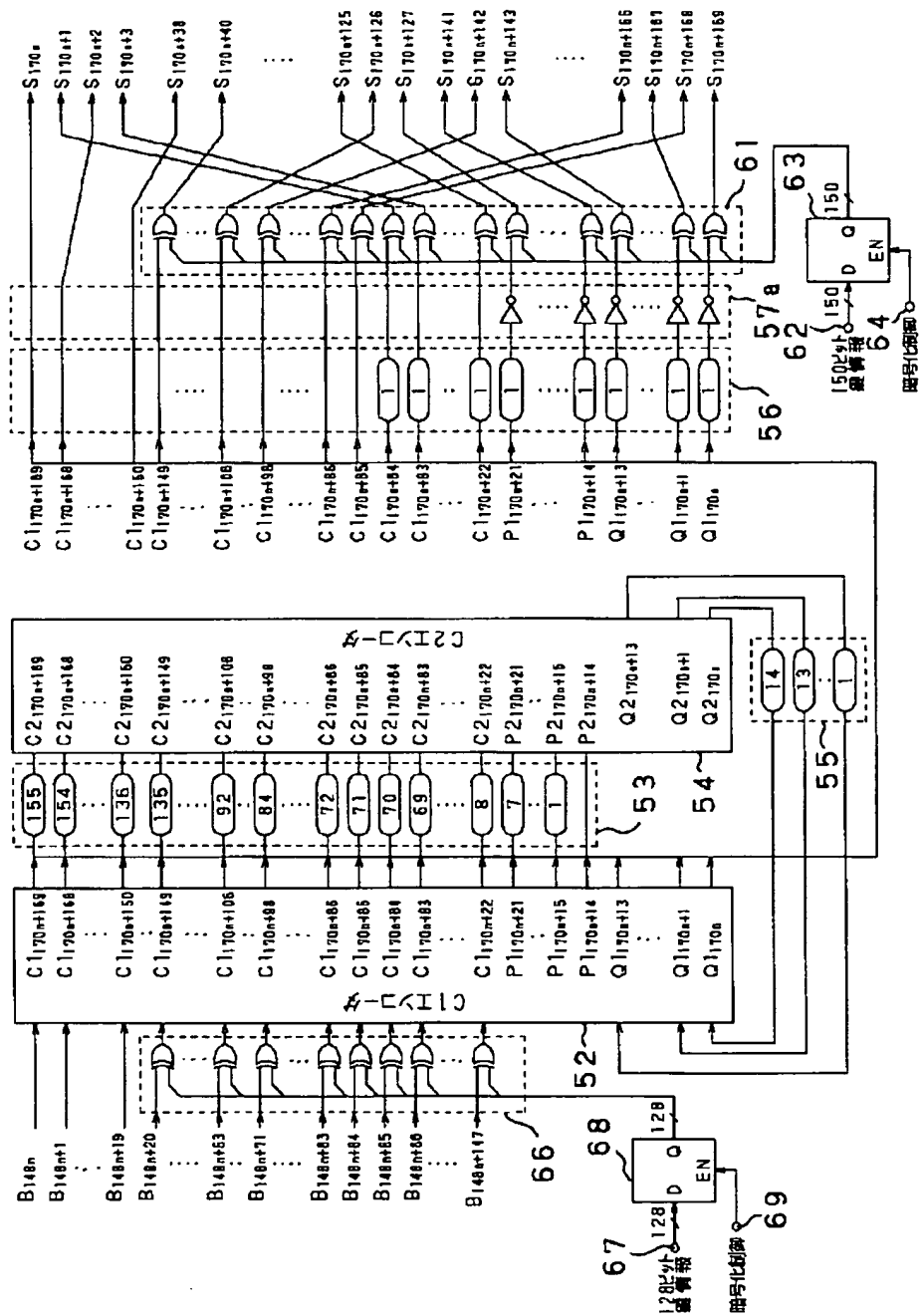
【図8】



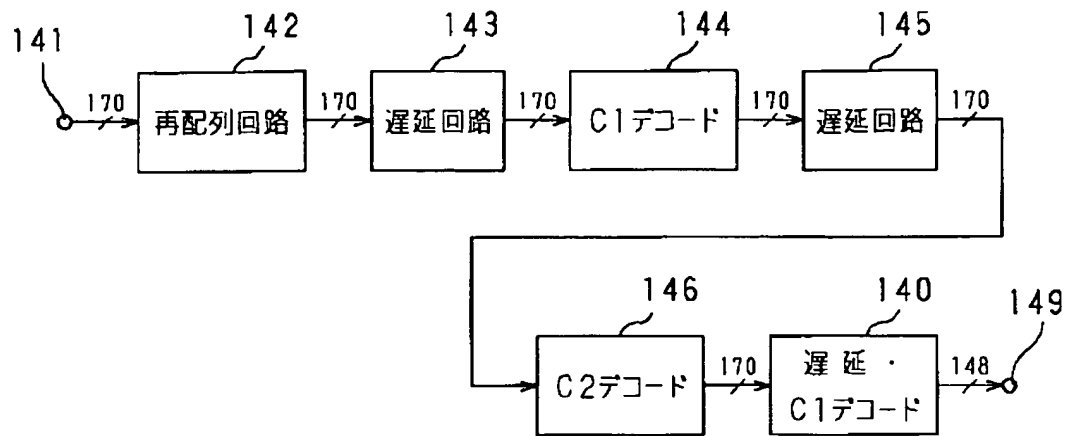
【図9】



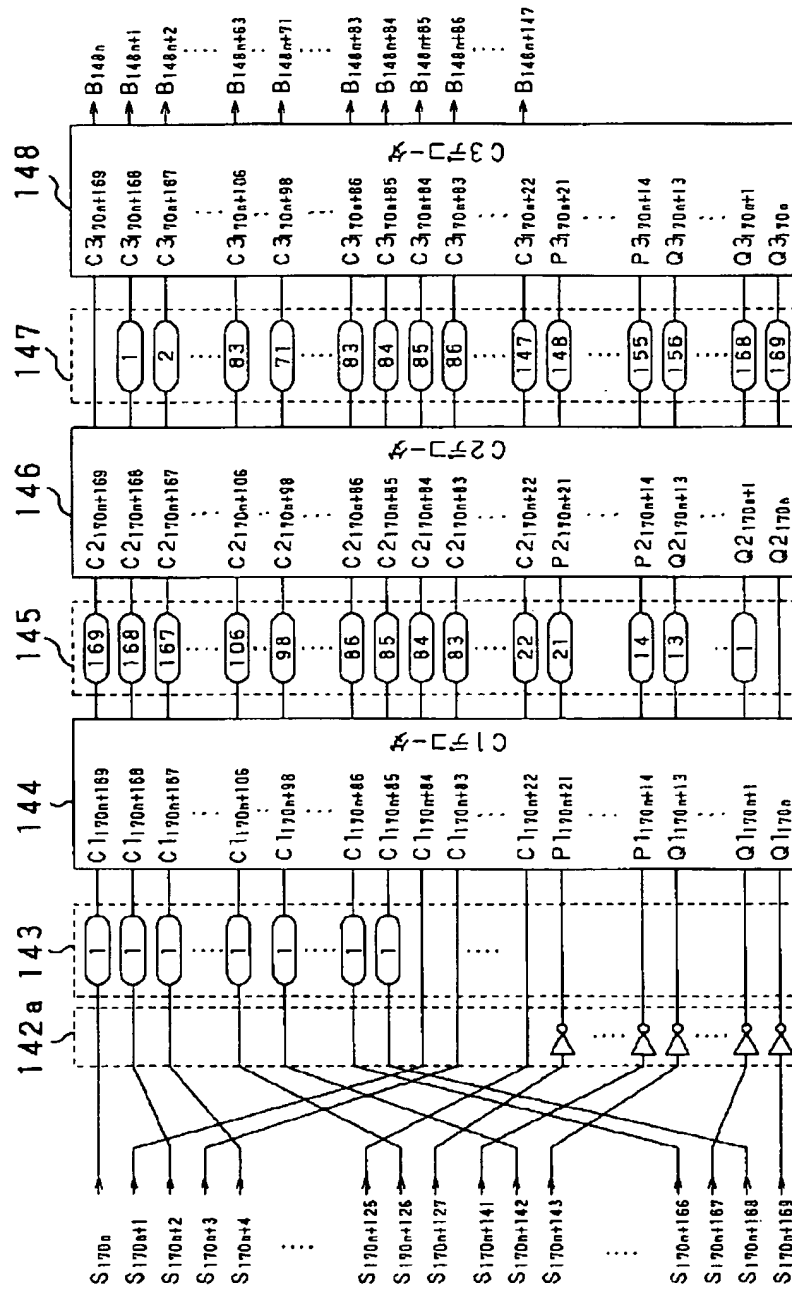
【図6】



【図10】



【図11】



5/13/05, EAST Version: 2.0.1.4